Technical Cybersecurity

NMAP

What is NMAP?

Network MAPper

- Written by Gordon Lyon (Fyodor), 1997
- Currently maintained and extend by the NMAP project
  - https://nmap.org

Various Approaches

- Uses various packet types and strategies
- Extensible via scripting

Wide variety of platforms

- Started on Linux, now available on just about anything

NMAP Strategy

First: Discovery

- What hosts are available
- Networks are frequently sparse
- **May not find all hosts!** Check out DNS, other techniques

Second: Recon

- Look at individual hosts, see what's running

Third: Details

- Detailed scan of hosts that look intriguing

Getting Caught

NMAP USED IN A VARIETY OF DOMAINS

- Penetration testers
- Hackers
- Network Administrators

EXPOSURE DEPENDS ON YOUR ROLE

- Pentest? Maybe okay depending on rules of engagement
- Hackers? Generally *not* okay to be obvious
- Admins? Don’t care

Fast or Slow, Loud or Silent

Nmap options support various needs

- …it doesn't have a loud option per se, but some techniques are easier for defenders to see than others
- …and some techniques are less likely to succeed than others

Engagement roles

- Sometimes you just don't have time
- Evaluate the risk

Proxies

Nmap supports proxies

- Very important!
- Pivoting
- Inaccessible subnets
- Hiding attribution

Sources can be found even with proxies

- …technically, that is
- It gives you more time
- Hard enough to get logs from networking staff
- Getting information from another company? forget it.

Let’s build our lab so we can get started.